EXHIBIT A

Joint Motion of Defendants ISS & Symantec for Summary Judgment of Invalidity Pursuant to 35 U.S.C. §§ 102 & 103 (D.I. 297)

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	Civil Action No. 04-CV-1199 (SLR)

JOINT MOTION OF DEFENDANTS ISS AND SYMANTEC FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103

Pursuant to the Court's June 30, 2005 Scheduling Order, Defendants Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively "ISS") and Symantec Corporation, a Delaware corporation ("Symantec"), move pursuant to Fed. R. Civ. P. 56, for an Order granting summary judgment that the asserted claims of the four patents-in-suit assigned to Plaintiff SRI International ("SRI") are invalid under 35 U.S.C. §§ 102 and 103.

Dated: June 16, 2006

POTTER ANDERSON & CORROON LLP

/s/ Richard L. Horwitz
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192
rhorwitz@potteranderson.com
dmoore@potteranderson.com

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600
Fax: (404) 572-51345

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation

MORRIS, JAMES, HITCHENS &
WILLIAMS, LLP

/s/ Mary B. Matterer
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID &
BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on the 16th day of June, 2006, I electronically filed the foregoing document, **JOINT MOTION OF DEFENDANTS ISS AND SYMANTEC FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103,** with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 16th day of June, 2006, the foregoing document was served via email and via federal express on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
1180 Peachtree Street
Atlanta, GA 30309-3521
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/Mary B. Matterer
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com
Counsel for Defendant Symantec Corporation

EXHIBIT B

Excerpts from Opening Brief in Support of Joint Motion for Summary Judgment of Invalidity Pursuant to 35 U.S.C. §§ 102 & 103 of Defendants ISS and Symantec (D.I. 299)

FILED UNDER SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation,

Plaintiff and
Counterclaim-Defendant,

v.

INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs.

Civil Action No. 04-CV-1199 (SLR)

OPENING BRIEF IN SUPPORT OF JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103 OF DEFENDANTS ISS AND SYMANTEC

Richard L. Horwitz (#2246)
David E. Moore (#3983)
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:
Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600
Fax: (404) 572-5134

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
MORRIS, JAMES, HITCHENS
& WILLIAMS, LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800

OF COUNSEL:
Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID &
BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

Table of Contents

REDACTED

I. STATEMENT OF THE CASE

In this action, SRI International, Inc. ("SRI") has sued Defendants Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively "ISS") and Symantec Corporation, a Delaware corporation ("Symantec") for patent infringement.[1] At issue are four patents relating to network intrusion detection.[2] All of the patents-in-suit claim the same priority date of November 9, 1998 and all share an almost identical written disclosure. Phillip Porras and Alfonso Valdes, employees of SRI, are the named inventors on all four patents.

The patents-in-suit generally relate to detecting attacks on computer networks, a field known as intrusion detection. There are two main facets to the patents-in-suit: (1) a hierarchy of monitors for detecting suspicious network activity, and (2) a statistical algorithm for use in detecting attacks. The '338 claims focus upon the statistical algorithm, the '203 and '615 claims focus upon the hierarchical monitor architecture, and the '212 claims include both facets.

These patents result from SRI's work on a system called EMERALD, which was funded by the United States government under the auspices of the Defense Advanced Research Projects Agency ("DARPA"). DARPA funded several projects on intrusion detection during the early-to-mid 1990s. In addition to EMERALD, DARPA also funded

[1] All referenced exhibits are attached to the Declaration of Renee DuBord Brown.

[2] The patents-in-suit are U.S. Patent Nos. 6,321,338 ("the '338 patent") [Ex. A]; 6,708,212 ("the '212 patent") [Ex. B]; 6,484,203 ("the '203 patent") [Ex. C]; and 6,711,615 ("the '615 patent") [Ex. D]. SRI has asserted different sets of claims against each Defendant. For convenience, the superset of asserted claims is addressed herein, which encompasses: '338 claims 1-2, 4-5, 11-13, 18-19, 24; '212 all claims (SRI has not asserted this patent against ISS, however, ISS seeks a declaratory judgment that the patent is not infringed and is invalid); '203 claims 1-9, 11-20, 22; '615 claims 1-10, 12-21, 23, 34-41, 43-51, 53. Both Defendants are currently contesting the belated attempt by SRI to add '615 claims 74 and 78, and those claims are not discussed herein.

a system called JiNao, which was developed at North Carolina State University and an associated company called MCNC. The named inventors of the patents-in-suit collaborated on JiNao. Both EMERALD and JiNao adopted a statistical algorithm that had been developed at SRI in the late 1980s/early 1990s. Both EMERALD and JiNao applied this algorithm to network traffic data. Both EMERALD and JiNao employed hierarchical network monitors.

During the course of their work on EMERALD and JiNao, the researchers shared the fruits of their government-funded research with the public by publishing detailed papers describing these systems. These public disclosures pre-date the priority filing date of the patents-in-suit by more than one year and describe all elements of the patent claims at issue. As a result, these printed publications invalidate the claims-in-suit.

SRI is not entitled to patent claims that would exclude others from practicing what had already been placed in the public domain. Under 35 U.S.C. § 102 (b), a patent is invalid if it claims inventions that were described in a printed publication more than one year before the filing date of the patent application. This rule applies equally to any public disclosure – including prior disclosures by the very person who later seeks a patent. The patent laws are designed to promote technological advances, not takings from the public domain. *See Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 148-49 (1989). If an inventor shares his invention with the public and does not file for patent protection within one year, the invention is dedicated to the public. Here, the named inventors filed their patent application in November 1998, but described the claimed subject matter in at least two publications dated more than one year before that filing date. In addition, the developers of the JiNao system also published their paper describing the claimed subject matter more than one year before that filing date. The inventors are therefore not entitled to patents on these claims.

The first publication by one of the named inventors, Mr. Porras, was published and presented at a national conference in October 1997. *See* P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20th National Information Systems Security Conference, October 7, 1997 ("*Emerald 1997*") [Ex. E]. This paper disclosed SRI's EMERALD project, which built upon earlier, well-known work at SRI. This paper presented the same hierarchical architecture and statistical analysis algorithms as disclosed and claimed in the patents-in-suit. The similarity between the patent specification and the *Emerald 1997* paper is striking. Entire figures and paragraphs from this paper were copied verbatim into SRI's later-filed patent specification. Even the inventors and SRI's own expert have admitted that *Emerald 1997* describes all or substantial portions of the elements of the claims of the '212, '203, and '615 patents. SRI has advanced a makeweight argument that this paper is not enabling in a belated attempt to distinguish *Emerald 1997* from the claims of the patents-in-suit. Because the patent and the paper are described at the same level of detail, these arguments simply do not rise to the level of a genuine issue of material fact and, therefore, can and should be resolved as a matter of law on summary judgment.

REDACTED

REDACTED

Resolution of this case in its entirety on summary judgment is appropriate. The text of the printed publications upon which Defendants rely cannot be disputed. The dates of publication of these prior art references are beyond genuine dispute. The similarity, if not identity, of the description between these prior art publications and the patents-in-suit can also not be genuinely disputed, and have been largely conceded by the inventors and SRI's expert. In the case of *Emerald 1997* and *Live Traffic*, the prior art publications were authored by the inventors themselves to describe the very same intrusion detection system – EMERALD – described in the specification of the patents-

REDACTED

in-suit.[4]

REDACTED

Furthermore, this summary judgment motion does not in any way rest upon the outcome of the claim construction in this case. This unique situation is due to the fact that *Emerald 1997* and *Live Traffic* were written by the inventors about the same system discussed in the patents-in-suit, and thus the language used is virtually identical.

REDACTED

Thus, the references relied upon herein are invalidating references regardless of whether SRI's or the Defendant's proposed constructions are adopted.

II. SUMMARY OF THE ARGUMENT

REDACTED

2. In the alternative, *Emerald 1997* in combination with *Intrusive Activity 1991* renders obvious pursuant to 35 U.S.C. § 103 the '203 and '615 asserted claims.

REDACTED

[4] To the extent there are claims with limitations that are not explicitly described in the references, those limitations would have been inherent in the disclosure or obvious additions to that disclosure. Indeed, the named inventors themselves pointed to combining EMERALD with the additional reference relied upon herein for the obviousness showing of certain limitations: L.T. Heberlein et al., *A Method to Detect Intrusive Activity in a Networked Environment*, 14th National Computer Security Conference, Oct. 1-4, 1991 ("*Intrusive Activity 1991*") [Ex. F].

REDACTED

III. STATEMENT OF FACTS

A. Background Regarding Intrusion Detection

1. The history of the intrusion detection field

Intrusion detection systems ("IDS") are designed to detect, and in some cases thwart, unwanted attempts to infiltrate or access a computer or computer network. An "intrusion" can refer to any type of anomalous, illicit, or prohibited activity. An intrusion may originate from an external threat, or misuse by an internal user. IDS has been described as "a burglar alarm for computers and networks." R. Bace, Intrusion Detection at 7 (Macmillan Technical Publishing 2000) [Ex. Z]. Like any technology, the IDS field has evolved over time. In order to provide a context for understanding the claimed inventions, this section provides a short overview of the history of the IDS field.

The U.S. government has played an important role. Beginning in the 1970's, the Department of Defense ("DOD") funded a "trusted systems" initiative to provide computer system security for the processing of classified information. As part of this program, the DOD created a policy for implementing certain auditing functions for computers to track behavior and discover potential security problems. *See* R. Bace, Intrusion Detection at 11 [Ex. Z]. An audit trail (also known as an "audit log") is a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. An audit trail may track basic operating system functions, such as system calls and processes performed, or it may track application usage or data access.[5]

[5] For an overview regarding audit trails, *see* S. Garfinkel and G. Spafford, Practical

Many early IDS systems focused upon the analysis of audit trail information. Such analysis is sometimes referred to as "host-based" because it relies upon information generated on a particular "host" or computer. However, with the proliferation of large computer networks and the likelihood of network-based attacks increasing, IDS systems began focusing upon network traffic and network sources for attack. For example, in the early 1990's, the Network Security Monitor ("NSM") developed at the University of California at Davis targeted computer networks and analyzed packet data. *See id.* at 18-19 [Ex. Z]; L.T. Heberlein et al., *A Network Security Monitor,* Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, at 296-304, Oakland, C.A., May 7-9, 1990 [Ex. NN].

As the inventors of the patents-in-suit have acknowledged, analysis of packet data in the context of network monitoring is quite old, and has been studied extensively in both the IDS field and many other areas of computing.[6] Packet-switched networks were first developed by the DOD for the Advanced Research Projects Agency Network ("ARPANET") in the late 1960s, which eventually formed the backbone of the Internet we know today. In the 1970-80s, early Internet researchers began developing a standard communication protocol for the Internet. This protocol suite became known as TCP/IP ("Transmission Control Protocol/Internet Protocol").[7]

UNIX & INTERNET SECURITY at 289-92 (O'Reilly and Assoc. 2nd ed. 1996) [Ex. AA].

[6] The inventors have stated in their publications that the concepts of network monitoring and the use of packet monitoring in IDS were not new at the time of the alleged inventions. *See* P. Porras and A. Valdes, *Live Traffic* at 3 (noting that "[n]etwork monitoring, in the context of fault detection and diagnosis for computer network and telecommunication environments, has been studied extensively by the network management and alarm correlation community" and "[b]oth [the NSM and NADIR systems] performed broadcast LAN packet monitoring to analyze traffic patterns for known hostile or anomalous activity") [Ex. I].

[7] *See* B. M. Leiner et al., A Brief History of the Internet,

In conjunction with the growth of the Internet, a wide variety of different types of computer and networking hardware were developed to handle the routing, monitoring, and filtering of network traffic and network packets. For example, routers and gateways were developed to connect computer networks. Routers and gateways receive packets and forward them to their correct destinations based upon the address in each packet's header.[8] As the need for securing networks, especially those connected across the Internet, became apparent, "firewalls" were developed in the early 1990's to provide a mechanism to filter and block unwanted packets and traffic.[9] Firewalls and the information they generate serve as important data sources for IDS systems.[10]

2. History of SRI's IDES, NIDES and EMERALD projects

SRI, in conjunction with various government research efforts, has worked and published in the IDS field for more than 20 years. Much of this published work involves a system that has undergone three different evolutions over time: IDES, NIDES, and EMERALD. As the inventors themselves have explained:

> Our earlier intrusion-detection efforts in developing IDES (Intrusion Detection Expert System) and later NIDES (Next-Generation Intrusion Detection Expert System) were oriented toward the surveillance of user-session and host-layer activity. This previous focus on session activity within host boundaries is understandable given that the primary input to intrusion-detection tools, audit data, is produced by mechanisms that tend

http://www.isoc.org/internet/history/brief.shtml (last visited June 15, 2006).

[8] Although these two terms have been used synonymously, a gateway has also been defined as connecting networks using different communication protocols. *See* definitions of "router" and "gateway" in COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997) [Ex. LL].

[9] *See* Avolio Decl., ¶ 24 [Ex. X].

[10] "Many firewalls, I&A systems, access control systems, and other security devices and subsystems generate their own activity logs. These logs contain information that is, by definition, of security significance; they are therefore of particular value to the intrusion detection process. Including these logs as information sources is an obvious way to improve the quality of the intrusion detection process." R. Bace, INTRUSION DETECTION at 74 [Ex. Z].

> to be locally administered within a single host, or domain. However, as the importance of network security has grown, so too has the need to expand intrusion-detection technology to address network infrastructure and services. In our current research effort, EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances), we explore the extension of our intrusion-detection methods to the analysis of network activity.

Live Traffic at 3 [Ex. I]. Different authors at SRI, including the named inventors for the patents-in-suit, published extensively on IDES, NIDES, and EMERALD prior to filing the '338 patent.[11]

In the late 1980s, SRI began working on IDES – a system to observe computer behavior and learn to recognize "normal" behavior and deviations from normal behavior. *See* H. Javitz and A. Valdes, *The SRI IDES Statistical Anomaly Detector*, 1991 IEEE Computer Society Symposium on Research in Security and Privacy (May 1991) [Ex. GG]. The statistical anomaly detection algorithm used by SRI in all of its IDS work was developed as part of IDES. SRI's "next-generation" of the IDES project, NIDES, furthered this work. *See* R. Jagannathan et al. (including A. Valdes), *System Design Document: Next-Generation Intrusion Detection Expert System (NIDES)*, March 9, 1993 at 55 [Ex. HH]. NIDES used the IDES statistical profiling algorithms to monitor computer information for deviations from normal computer activity. NIDES also included the use of a rule (or signature) based expert system to detect known attacks. *Id.* at 2-4, 31 [Ex. HH]. NIDES had a modular architecture that included two analysis engines (statistical and signature) and a resolver to combine the results of the two engines. *Id.* at 2-4 [Ex. HH].

IDES and the original NIDES were primarily host-based systems, deriving their information from audit data. As the use of networking expanded and other intrusion

[11] *See* Ex. N, listing many different SRI publications on IDES, NIDES, and EMERALD,

detection systems began to look at network traffic and large networks, SRI sought government funding to create a successor to NIDES that would monitor network traffic. This system was eventually called EMERALD.

By December 1996, SRI had published a conceptual overview of the EMERALD system, *see* P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, Conceptual Overview,* http://www.sdl.sri.com/papers/emerald-position1/ (December 18, 1996) [Ex. JJ], and by October 1997, SRI had fully disclosed the EMERALD system in the *Emerald 1997* publication. Like NIDES, EMERALD employed a modular component architecture called a "monitor" that included a statistical profiling engine and a signature-based engine with a resolver to combine the results from the two engines.

The *Emerald 1997* paper disclosed the details of the analysis hierarchy of monitors and the statistical detection method claimed in the patents-in-suit. Indeed, the similarities between *Emerald 1997* and the common patent specification are extensive. For example, Fig. 1 from *Emerald 1997* is virtually identical to the patents' Fig. 2.[12] In addition, Fig. 2 from *Emerald 1997* is identical to the patents' Fig. 3.[13] There are numerous examples in which the language of *Emerald 1997* can be found verbatim in the patents' specification.[14] Both *Emerald 1997* and the patents-in-suit also state that they were funded by the same contract from DARPA.[15]

all dated more than one year prior to November 9, 1998.

[12] *Compare Emerald 1997*, Fig. 1 at p. 357, with '338 Fig. 2 and col. 3:4-5.

[13] *Compare Emerald 1997*, Fig. 2 at p. 358, with '338 Fig. 3 and col. 3:6-7.

[14] *See* comparison of *Emerald 1997* to '338 common patent specification [Ex. W].

[15] DARPA contract F30602-96-C-0294.

All three of the "hierarchical" patents ('212, '203 and '615) are extremely redundant.[24] The '203 patent claims focus on the analysis hierarchy of monitors for detecting suspicious network activity. The '203 patent requires that at least one type of particular "network traffic data categories" be used for the analysis. The '203 patent does not require any particular detection method (*i.e.*, the suspicious network activity may be detected using either statistical or signature methods). Claim 1 is representative of the alleged invention claimed:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:
>
> deploying a plurality of network monitors in the enterprise network;
>
> detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};[25]
>
> generating, by the monitors, reports of said suspicious activity; and
>
> automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

The '615 claims are almost exactly the same as the '203 claims. '615 claim 1 merely adds two additional categories of network traffic data: "network connection acknowledgments" and "network packets indicative of well-known network-service protocols."

The '212 claims are also very similar to the '203 and '615 claims. The '212 claims do not require use of any of the particular "network traffic data categories" from '203 claim 1. Instead, the '212 claims require that at least one of the network monitors

[24] *See* Ex. CC, which compares claim 1 of the '212, '203, and '615 patents, and highlights the two limitations where these claims differ.

[25] In order to invalidate this limitation, a prior art reference need only disclose one of the claimed "network traffic data" categories.

utilize a "statistical detection method." In addition, '212 claims 2 and 3 further require the use of a "signature matching detection method."

D. THE SUMMARY OF ESTABLISHED FACTS

1. The priority filing date for all of the patents-in-suit is November 9, 1998.
2. *Emerald 1997* was publicly available more than one year prior to November 9, 1998.[26]

REDACTED

7. *Emerald 1997* discloses all of the limitations of the '212 asserted claims.[31]
8. *Emerald 1997* discloses monitoring network datagrams (a synonym for network packets).[32]

[26] SRI has admitted that *Emerald 1997* was published on October 9, 1997. *See* Plaintiff SRI's Responses to Defendant ISS's First Set of Requests for Admission, Request No. 1 [Ex. O].

REDACTED

[29] SRI has admitted that *Intrusive Activity 1991* was publicly available prior to November 1997, *see* SRI's Responses to Symantec's Third Set of Requests for Admission [Ex. P].

REDACTED

[31] Valdes Tr. 466-67 [Ex. U]; chart comparing *Emerald 1997* to '212, '203, and '615 asserted claims [Ex. K]; *see also supra* Part IV.B.1.

[32] Emerald 1997 at 356.

REDACTED

12. One of ordinary skill in the art would have been motivated to combine *Emerald 1997* with its cited reference *Intrusive Activity 1991* to determine what measures of network datagrams/packets to monitor.[36]

13. *Intrusive Activity 1991* discloses analysis of "network packet data volume," "network connection requests," and "network connection denials."[37]

14. *Emerald 1997* alone and in combination *with Intrusive Activity 1991* discloses all of the limitations of the asserted '203 and '615 claims.[38]

15. *Emerald 1997* is an enabling reference for the asserted claims of the '212, '203, and '615 patents.[39]

REDACTED

REDACTED

[36] Kesidis Tr. 673-76 [Ex. V]; *see also supra* Part IV.B.2.b.

[37] *Intrusive Activity 1991* at 368-69, 365, 370 [Ex. F]; *see also supra* Part IV.B.2.b.

[38] Chart comparing *Emerald 1997* to '212, '203, and '615 asserted claims [Ex. K]; *see also supra* Part IV.B.2.

[39] Heberlein Decl. ¶¶ 86-93 [Ex. Y].

REDACTED

REDACTED

IV. SUMMARY JUDGMENT OF INVALIDITY SHOULD BE ENTERED ON ALL OF THE ASSERTED CLAIMS

A. LEGAL STANDARDS

1. Summary judgment

Summary judgment is appropriate if "no genuine issue exists as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). "Facts that could alter the outcome are material, and disputes are genuine if evidence exists from which a rational person could conclude that the position of the person with the burden of proof on the disputed issue is correct." *Matsushita Elec. Indus. Co. v. Cinram Int'l, Inc.*, 299 F. Supp. 2d 348, 357 (D. Del. 2004) (citations omitted). The moving party bears the burden of proving that no genuine issue of material fact exists. *See Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 n.10 (1986). If the moving party proves an absence of material fact, the nonmoving party "must come forward with 'specific facts showing that there is a genuine issue for trial.'" *Matsushita*, 475 U.S. at 587 (quoting Fed. R. Civ. P. 56(e)).

REDACTED

REDACTED

REDACTED

Where the reference has previously been considered by the US PTO Examiner, an element of deference is given to the decision of the examiner. *American Hoist & Derrick Co. v. Sowa & Sons, Inc.* 725 F.2d 1350, 1358-59 (Fed. Cir. 1984). However, the law recognizes that there are references previously considered by an Examiner which contain "disclosure so poignantly impacting upon patentability as to render virtually irrelevant the fact of its consideration by the examiner." *Lear Siegler, Inc. v. Aeroquip Corp.*, 733 F.2d 881, 886 n.4 (Fed. Cir. 1984). Given the closeness of the *Emerald 1997* and *Live Traffic* disclosures to the claims of the patents in question (including complete identity of several figures), the overlap in authorship, and the Examiner's complete silence on all prior art issues during prosecution of all of the patents-in-suit, *Emerald 1997* and *Live*

Traffic are such references.[45]

REDACTED

[45] The Examiner did not issue a single Office Action on any piece of prior art for any of the four patents-in-suit.

REDACTED

REDACTED

3. Obviousness under 35 U.S.C. § 103

A patent claim is invalid for obviousness under 35 U.S.C. § 103 if the differences between it and the prior art are such that the claimed subject matter as a whole would have been obvious to one of ordinary skill in the art at the time the invention was made. *See Union Carbide Plastics & Tech. Corp. v. Shell Oil Co.*, 308 F.3d 1167, 1187 (Fed. Cir. 2002). The ultimate determination of whether an invention would have been obvious is a legal conclusion based on the totality of the evidence, including underlying factual inquires. *See Tegal Corp. v. Tokyo Electron America, Inc.*, 257 F.3d 1331, 1348 (Fed. Cir. 2001). There are typically four underlying factual inquiries: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) any objective indicators of non-obviousness, more commonly termed secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966); *B.F. Goodrich Co. v. Aircraft Braking Sys. Corp.*, 72 F. 3d 1577, 1582 (Fed. Cir. 1996). Where a legal conclusion of obviousness is disputed, but the underlying facts are not, there is no issue of fact requiring a trial and summary judgment is appropriate. *See Newell Cos. v. Kenney Mfg. Co.*, 864 F. 2d 757, 763 (Fed. Cir. 1988). In addition, summary judgment on the basis of obviousness may be granted to invalidate patent claims when the subject matter of the invention and the prior art are so readily understandable as to eliminate any genuine issue of fact. *See Union Carbide Corp. v. American Can Co.*, 724 F.2d 1567, 1573 (Fed. Cir. 1984).

The existence of each limitation of a claim in the prior art does not, by itself, demonstrate obviousness. Instead, there must be a "reason, suggestion, or motivation" to combine the references. *Smiths Indus. Med. Sys., Inc. v. Vital Signs, Inc.*, 183 F. 3d 1347, 1353 (Fed. Cir. 1999).

> [T]he motivation-suggestion-teaching test asks not merely what the references disclose, but whether a person of ordinary skill in the art, possessed with the understandings and knowledge reflected in the prior art, and motivated by the general problem facing the inventor, would have been led to make the combination recited in the claims.

In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006). Obviousness can be found on the basis of a "problem [that] was within the general knowledge of those of ordinary skill in the art," even if the patent is not directed at "the identical problem addressed in [the] prior art." *Cross Medical Products, Inc. v. Medtronic Sofamor Danek, Inc.*, 424 F.3d 1293, 1322-23 (Fed. Cir. 2005).

B. Emerald 1997 Anticipates and Renders Obvious the Asserted Claims

Emerald 1997 expressly anticipates or inherently anticipates all of the asserted claims of the '212, '203, and '615 "hierarchical" patents. In addition, *Emerald 1997* in combination with an internally-cited reference also renders obvious the asserted claims of the '203 and '615 patents. The chart at Exhibit K provides the relevant disclosures from *Emerald 1997* for both anticipation and obviousness for each of the claim limitations.

This is a somewhat unusual case in that Alfonso Valdes, a named inventor, admitted that *Emerald 1997* disclosed the claimed invention of '212 claim 1:

REDACTED

REDACTED

Mr. Valdes thus also admitted that all of the same elements of the '203 and '615 patent claims were present in *Emerald 1997*. The only additional limitation in these claims is the limitation of particular "categories" of network traffic (only *one* of which needs to be disclosed in order for a prior art reference to anticipate). But those limitations were inherently disclosed in *Emerald 1997* to one of ordinary skill in the art, or, at a minimum, would have been obvious in light of the express teaching in *Emerald 1997* to analyze those network traffic categories based upon the cited reference *Intrusive Activity 1991*.

While *Emerald 1997* was submitted to the Examiner during the prosecution of the '338, '212 and '615 patents, it was not considered during the '203 prosecution.[48] However, given the substantial overlap in text and figures between *Emerald 1997* and the patents' specification, as well as numerous admissions from SRI's inventors and expert, this reference so clearly impacts upon patentability that this fact should be considered virtually irrelevant.

1. Emerald 1997 describes all of the claimed inventions of the '212 patent

The overlap in figures and text between *Emerald 1997* and the patents' specification is striking, as shown in Exhibit W. Since '212 claim 1 is representative of many of the limitations present in the '203, '212 and '615 claims, a comparison of its limitations with the disclosure in *Emerald 1997* is instructive:[49]

[47] Valdes Tr. 466-67 [Ex. U]. *See also* admissions of SRI's expert Dr. Kesidis regarding *Emerald 1997* and the limitations of the hierarchical patent claims: Kesidis Tr. 670-72 (*Emerald 1997* discloses using network datagrams / IP packets for intrusion detection); 690-93 (*Emerald 1997* teaches deploying a plurality of monitors); 693-94 (*Emerald 1997* monitors generate reports of intrusions) [Ex. V].

[48] Kunin Decl. ¶¶ 17-19 [Ex. BB].

[49] The citations below are merely representative, and additional relevant quotes are

'212 Claim 1	Disclosure in *Emerald 1997* (emphasis added) (*see also* Exhibit K).
Method for monitoring an enterprise network, said method comprising the steps of:	EMERALD introduces a highly distributed, building-block approach to **network surveillance**, attack isolation, and **automated** response. *Emerald 1997* at 353. The typical target environment of the EMERALD project is a large **enterprise network** with thousands of users connected in a federation of independent administrative domains. *Id.* at 354.
deploying a plurality of network monitors in the enterprise network;	Service monitors are dynamically deployed within a domain... *Id.* at 355. All EMERALD monitors (service, domain, and enterprise) are implemented using the same monitor code base. *Id.* at 357. The basic analysis unit in this architecture is the EMERALD monitor, which incorporates both signature analysis and statistical profiling. *Id.* at 364.
detecting, by the network monitors, suspicious network activity	Multiple analysis engines implementing different analysis methods may be employed to **analyze a variety of event streams** that pertain to the same analysis target... The profiler and signature engines receive large volumes of event logs specific to the analysis target, and produce smaller volumes of **intrusion or suspicion reports** that are then fed to their associated resolver. *Id.* at 356.
based on analysis of network traffic data,	Underlying the deployment of an EMERALD monitor is the selection of a target-specific event stream. **The event stream may be derived from** a variety of sources including audit data, **network datagrams,** [50] SNMP **traffic,** application logs, and analysis results from other intrusion-detection instrumentation. ... Event records are then forwarded to the monitor's analysis engine(s) for processing. *Id.* at 356. EMERALD also extends the statistical-profile model of NIDES, to analyze the operation of network services, network infrastructure, and activity reports from other EMERALD monitors. ... the Network Security Monitor [7] seeks to analyze packet data rather than conventional audit trails... More recent work in UC Davis' GrIDS effort [24] employs activity graphs of network operations to search for traffic patterns that may indicate network-wide coordinated attacks. *Id.* at 364.
wherein at least one of the network monitors utilizes a statistical detection	EMERALD's profiler engine performs **statistical profile-based anomaly detection** given a generalized event stream of an analysis target (Section III-C). *Id.* at 356.

included in Exhibit K.

[50] As SRI's expert has admitted, a datagram is equivalent to a packet. Kesidis Tr. 670-72 [Ex. V].

'212 Claim 1	**Disclosure in *Emerald 1997*** (emphasis added) (*see also* **Exhibit K**)
method;	
generating, by the monitors, reports of said suspicious activity; and	EMERALD employs a building-block architectural strategy using independent distributed surveillance monitors that can **analyze and respond to malicious activity** on local targets, and can interoperate to form an analysis hierarchy. *Id.* at 355. The profiler and signature engines receive large volumes of event logs specific to the analysis target, and produce smaller volumes of **intrusion or suspicion reports** that are then fed to their associated resolver. *Id.* at 356.
automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	***Domain monitors*** **correlate intrusion reports disseminated by individual service monitors,** providing a domain-wide perspective of malicious activity (or patterns of activity). ... **Enterprise-layer monitors correlate activity reports produced across the set of monitored domains....** Through this **correlation and sharing of analysis results,** reports of problems found by one monitor may propagate to other monitors throughout the network. *Id.* at 356.

As detailed in the charts attached in Exhibit K, all of the dependent claim limitations for the '212 patent are also disclosed in *Emerald 1997*. Thus, the '212 patent is anticipated and therefore invalid.[51]

2. Emerald 1997 renders obvious and/or inherently anticipates all of the asserted claims of the '203 and '615 patents

According to both inventors, the only limitation in '203 claim 1 that is not disclosed verbatim in *Emerald 1997* are the claimed network traffic data categories.[52] These categories are, however, inherently disclosed. They are also an obvious addition.

Both inventors admitted that they were not the first to monitor ***many*** of the claimed categories of network traffic data (only ***one*** of which is needed for a prior art system to be an invalidating reference).[53] The inventors simply monitored the same types

[51] As shown in Ex. K, a similar analysis applies for '615 independent claims 34 and 44.

[52] Porras Tr. 434-39 [Ex. T]; Valdes Tr. 459-60 [Ex. U].

[53] Porras Tr. 289-95; 444-54 [Ex. T]; Valdes Tr. 283-87 [Ex. U]; *see also* Kesidis Tr.

of network traffic other computer systems and intrusion detection systems were already monitoring. The listed types of network traffic are the same as those that were already in use by network entities and other intrusion detection systems in the early 1990s.[54] Thus, these categories would have been inherent and/or obvious from the disclosure in *Emerald 1997* of the data sources for such categories – network datagrams and logs kept by network infrastructure.

REDACTED

383-84 [Ex. V].

REDACTED

[54] Heberlein Decl. ¶¶ 53-58, 65-73 [Ex. Y].

REDACTED

REDACTED

b. Obvious to combine Emerald 1997 with an internally cited reference

Emerald 1997 explicitly states that the EMERALD system monitors "network datagrams" (known at the time to be network packets).[67] *Emerald 1997* goes on to explain that another intrusion detection system, the Network Security Monitor ("NSM"), also analyzed packet data, and directs the reader to a paper on NSM, cited reference [7]. *See Emerald 1997* at 364 [Ex. E], citing to L.T. Heberlein et al., *A Method to Detect Intrusive Activity in a Networked Environment*, 14th National Computer Security Conference, Oct. 1-4, 1991 ("*Intrusive Activity 1991*") [Ex. F]. SRI's expert Dr. Kesidis conceded that *Emerald 1997* directed one of skill in the art to look to the *Intrusive Activity 1991* reference to find out more about analyzing packet data.[68] Thus, *Emerald 1997* expressly provided the motivation to combine the two references. *See In re Saunders*, 444 F.2d 599, 603 (C.C.P.A. 1971) (sustaining an obviousness rejection involving the combination of an internally-cited reference, and noting "it would not have been necessary for one skilled in the art to have gone any further than another part of [the

REDACTED

[67] *Emerald 1997* at 356 [Ex. E]; Kesidis Tr. 670-72 [Ex. V].

[68] Kesidis Tr. 673-76 [Ex. V]; *see also* Porras Tr. 424-25 [Ex. T].

cited reference] to find the specified proportions of the appealed claims.").[69]

Like the patent specification's disclosure on abstracting raw network packet data into "events," *Intrusive Activity 1991* describes a method for analyzing network activity by developing representative "objects" from information in network packets. *See Intrusive Activity 1991* at 364 [Ex. F]. In particular, *Intrusive Activity 1991* defines parameters to monitor in a stream, or individual connection, composed of packets. *Id.* at 368 [Ex. F]. Two parameters explicitly called out are "the number of packets" and the "number of bytes" – both of which constitute a measure of "network packet data volume." *Id.* at 368-69 [Ex. F].[70] This is one of the network traffic categories listed in the '203 and '615 patent claims.

In addition, *Intrusive Activity 1991* discloses other measures listed in the claimed categories such as network connection requests and denials. For example, it explains that "network connections are ***created*** and ***destroyed*** continuously," *id.* at 365 (emphasis added) [Ex. F], and notes that:

> We have concentrated our analysis efforts on **isolated behavior-detection functions for connections.** ... The higher the suspicious value is, the more likely our monitor believes the connection is associated with intrusive activity. We monitored the Electrical Engineering and Computer Science LAN at UCD for a period of approximately three months. **During this time over 400,000 connections were detected and analyzed,** and among these connections, over 400 were identified as being associated with intrusive behavior.

[69] Some courts have held that internally-cited references satisfy anticipation as well, *see, e.g., Rheox, Inc. v. United Catalysts, Inc.*, 1995 U.S. Dist. LEXIS 13054 (D. N.J. 1995) (unpublished) (stating "consideration of a reference within a reference is consistent with the established standards for determining anticipation.") [Ex. PP].

[70] *See supra* note 63.

Id. at 370 (emphasis added) [Ex. F]. One of ordinary skill would have understood this disclosure of analyzing the creation and destruction of network connections to disclose monitoring "network connection requests" and "network connection denials."

Thus, *Emerald 1997* in combination *with Intrusive Activity 1991* renders obvious the claims of the '203 and '615 patents which require monitoring one or more particular categories of network traffic. As shown in Exhibit K, the rest of the dependent claim limitations for these patents are also disclosed in *Emerald 1997.*

3. Emerald 1997 is enabled

SRI suggests that *Emerald 1997* was merely a vague proposal that did not enable any of the claimed inventions.[71] But *Emerald 1997* is not a mere proposal – it is a detailed, peer-reviewed article published and presented at a conference proceeding. Given the striking similarities in detail between the patent specification and *Emerald 1997*,[72] SRI cannot simultaneously claim that the text in *Emerald 1997* is not enabling, while contending that the same text is enabling in the patent specification. If the patents-in-suit are enabled, so too is *Emerald 1997.*[73]

REDACTED

[71] Porras Tr. 433 (referring to *Emerald 1997* as an "early conceptual design") [Ex. T]; Kesidis Tr. 696 (describing *Emerald 1997* as a "research proposal") [Ex. V].

[72] *See* Ex. W.

[73] *See* Heberlein Decl. ¶¶ 89-93 [Ex. Y].

REDACTED

EXHIBIT C

Excerpts from Defendants' Joint Reply Brief in Support of Their Motion for Summary Judgment of Invalidity Pursuant to 35 U.S.C. §§ 102 & 103 (D.I. 400)

FILED UNDER SEAL

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	Civil Action No. 04-CV-1199 (SLR) **FILED UNDER SEAL** THIS DOCUMENT CONTAINS MATERIALS WHICH ARE CLAIMED TO BE CONFIDENTIAL AND COVERED BY A PROTECTIVE ORDER. THIS DOCUMENT SHALL NOT BE MADE AVAILABLE TO ANY PERSON OTHER THAN THE COURT AND OUTSIDE COUNSEL OF RECORD FOR THE PARTIES)

DEFENDANTS' JOINT REPLY BRIEF IN SUPPORT OF THEIR MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103

Richard K. Herrmann (#405)
Morris, James, Hitchens & Williams, LLP
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306
Tel: (302) 888-6800
Fax: (302) 571-1751

Attorneys for Defendant and Counterclaim Plaintiff Symantec Corporation

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)

Table of Contents

REDACTED

II. SUMMARY JUDGMENT OF INVALIDITY SHOULD BE ENTERED ON ALL OF THE ASSERTED CLAIMS

A. LEGAL STANDARDS

Summary judgment is appropriate here because SRI has failed to come forward with specific material facts showing a genuine issue for trial. "Facts that could alter the outcome are material, and disputes are genuine if evidence exists from which a rational person could conclude that the position of the person with the burden of proof on the disputed issue is correct." *Matsushita Elec. Indus. Co. v. Cinram Int'l, Inc.*, 299 F. Supp. 2d 348, 357 (D. Del. 2004) (citations omitted).

B. EMERALD 1997 ANTICIPATES AND RENDERS OBVIOUS THE ASSERTED CLAIMS

SRI concedes that *Emerald 1997* discloses all of the limitations of the '212 claims, and relies only on a vague "enablement" challenge. SRI also concedes that *Emerald 1997* explicitly discloses all but one of the limitations of the '203 and '615 claims, and challenges only the disclosure of the claimed "network traffic data" categories.

Given these admissions from SRI, its attempt to hide behind the presumption of validity makes no sense. The presumption of validity when a reference has been considered by the Examiner is rebuttable. *WMS Gaming Inc. v. Int.'l Game Tech.*, 184 F.3d 1339, 1355 (Fed. Cir. 1999). Defendants have overcome the presumption of validity, particularly in this case, where SRI has already *admitted Emerald 1997* discloses all of the limitations of the '212, and all but one of the limitations of the '203 and '615 patents.

As will be shown below, for the few issues SRI contests, Defendants have put forward clear and convincing evidence of invalidity, and SRI has failed to rebut it.[1]

REDACTED

[1] SRI has also failed to rebut Defendants' evidence that the Examiner in this instance failed to follow the MPEP and did not consider *Emerald 1997* during prosecution of the '203 patent. SRI cites nothing from the actual file history. *See* Opening Br. at 23 [D.I. 299], Res. Br. at 6-7 [D.I. 339].

REDACTED

REDACTED

3. Emerald 1997 and Intrusive Activity 1991 render the '203 and '615 claims obvious

The combination of *Emerald 1997* and *Intrusive Activity 1991* renders obvious the claims-in-suit of the '203 and '615 patents. *Intrusive Activity 1991*.[24] SRI has failed to raise any genuine issues of material fact to the contrary. First, SRI has not contested that *Intrusive Activity 1991* discloses monitoring network traffic data volume, one of the claimed network traffic data categories. SRI also fails to put forth the correct standard for a motivation to combine references. Under the correct standard, SRI's expert has admitted there was motivation to combine *Emerald 1997* and *Intrusive Activity 1991*, a point that SRI does not contest.[25] SRI's argument thus reduces to reliance upon secondary considerations of nonobviousness to avoid summary judgment. But the law is clear that secondary considerations do not preclude summary

REDACTED

[24] D.I. 301, Ex. F. Despite the fact that one of the inventors cited *Intrusive Activity 1991* in the *Emerald 1997* publication, this reference was never disclosed to the Examiner. Thus, the Examiner never considered this particular obviousness combination.

judgment in this instance.

First, SRI's Response Brief fails to even attempt to rebut that *Intrusive Activity 1991* discloses network packet data volume. The relevant disclosure is clearly called out in Defendants' Opening Brief, which states "[t]wo parameters explicitly called out are 'the number of packets' and the 'number of bytes' – both of which constitute a measure of 'network packet data volume.'"[26] Through its silence, SRI has implicitly admitted that *Intrusive Activity 1991* discloses monitoring "network packet data volume." Because disclosure of even one of the claimed categories of network traffic data is sufficient, SRI's silence means that it has conceded that all of the limitations of the '203 and '615 claims-at-issue are disclosed by the combination of *Emerald 1997* and *Intrusive Activity 1991*.[27]

SRI also attempts to argue that there was no motivation to combine *Intrusive Activity 1991* with *Emerald 1997*. SRI does not state the actual standard for motivation to combine, but instead appears to conflate it with the anticipation standard for incorporation by reference. For example, SRI states that "[a] person of ordinary skill attempting to practice the disclosure of *EMERALD 1997* would not be required to consult the *Intrusive Activity 1991* article."[28] That is far different from the actual standard for motivation to combine:

[25] *See infra* note 33 and accompanying text.

[26] Opening Br. at 31 [D.I. 299].

[27] SRI instead expends its energy only on attempting to demonstrate that additional disclosures in *Intrusive Activity 1991* do not disclose monitoring "network connection requests" and "network connection denials." SRI argues, without pointing to any support in the reference itself, that the Network Security Monitor (NSM), the system disclosed in *Intrusive Activity 1991*, only monitored "established connections." Res. Br. at 13 [D.I. 339]. But SRI's own expert has already disclaimed this argument in his deposition. When questioned, Dr. Kesidis was unable to point to any support for the notion that NSM monitored only established connections. Kesidis Tr. 619-37 at 629, 636-37 [7/10/06 Godfrey Decl. Ex. SS]. In any event, even if SRI had raised a genuine issue of material fact as to whether or not *Intrusive Activity 1991* discloses network connection requests and denials (which it has not) this is irrelevant in light of the fact that SRI has implicitly conceded that the reference discloses monitoring network packet data volume.

[28] Res. Br. at 12 [D.I. 339].

> [W]hether a person of ordinary skill in the art, possessed with the understandings and knowledge reflected in the prior art, and motivated by the general problem facing the inventor, would have been led to make the combination recited in the claims.

In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006).

While an explicit motivation to combine is not required, here Defendants have actually demonstrated such an explicit motivation in the *Emerald 1997* reference itself. *National Steel Car, Ltd., v. Canadian Pacific Railway, Ltd.*, 357 F.3d 1319, 1337 (Fed. Cir. 2004). The text of *Emerald 1997* states the *Intrusive Activity 1991* article relates to "analyz[ing] packet data" and further provides a citation to *Intrusive Activity 1991*.[29] *Emerald 1997* disclosed that network packets were a source of event data for the EMERALD system, and thus one of ordinary skill interested in learning more about how EMERALD performed network packet data monitoring would have been motivated to combine the teachings of *Intrusive Activity 1991*.[30]

SRI's expert ***agreed at his deposition*** that these facts established a motivation to combine the two references:

REDACTED

SRI never even mentions or discusses this admission from their own expert.

Instead, SRI attempts to distinguish *Application of Saunders*, 444 F.2d 599, 601 (C.C.P.A. 1971) from the situation at issue. SRI appears to suggest that because *Saunders* dealt with patents, and the references in this case are technical papers, somehow *Saunders* is

[29] *See Emerald 1997* at 364 and 365[7] [D.I. 301, Ex. E].

[30] *See Emerald 1997* at 356 [D.I. 301, Ex. E]. *See also* Kesidis Tr. 670-72 (admitting a network datagram is equivalent to a packet) [D.I. 301, Ex. V].

[31] Kesidis Tr. 675-76 [D.I. 301, Ex. V]; *see also* Porras Tr. 424-25 [7/10/06 Godfrey Decl. Ex.

irrelevant. SRI also appears to conflate a finding of a motivation to combine with the standard for incorporation by reference.[32] But Defendants merely cited to *In re Saunders* for the unsurprising notion that it is obvious to combine references where a first reference points to a second reference explicitly. SRI's analysis of minute distinctions between *Saunders* and the current situation do nothing to cast doubt upon this general concept. Indeed, as noted above, both SRI's expert and one of the inventors agreed that the facts in this case establish a motivation to combine the two references.[33]

The only additional argument made by SRI is that "there would be no motivation to consult such an outdated technical article in a rapidly evolving field such as network security."[34] SRI cites no law for the proposition that motivation to combine depends upon the age of a reference. Furthermore, *Intrusive Activity 1991* was not an "outdated" reference – it described NSM, the well-known earliest network intrusion detection system.[35] NSM has been widely acknowledged as groundbreaking work.[36] This argument by SRI only draws attention to the fact that monitoring the claimed network traffic categories was old – quite old, as *Intrusive Activity 1991* demonstrates, and as the inventors themselves have admitted.[37] It is unsurprising that the authors of *Emerald 1997* would cite to a reference describing one of the seminal works on network intrusion detection to provide further information on specific network traffic categories

RR].

[32] Res. Br. at 10-12 [D.I. 339].

[33] Kesidis Tr. 675-76 [D.I. 301, Ex. V]; *see also* Porras Tr. 424-25 [7/10/06 Godfrey Decl. Ex. RR].

[34] Res. Br. at 12 [D.I. 339].

[35] Porras Tr. 241-43 [7/10/06 Godfrey Decl. Ex. RR].

[36] *See*, e.g., R. Bace, INTRUSION DETECTION at 19-20 (stating "NSM was a significant milestone in intrusion detection research because it was the first attempt to extend intrusion detection to heterogeneous network environments.") [7/10/06 Godfrey Decl. Ex. YY].

[37] Porras Tr. 289-95, 444-54 [D.I. 301, Ex. T]; Valdes Tr. 283-87 [D.I. 301, Ex. U]; *see also* discussion in Defendant's Joint Opposition to SRI's Motion for Partial Summary Judgment of No Anticipation by the "EMERALD 1997" Publication at 10-11 [D.I. 342].

to monitor.

SRI's failure to rebut the concession from their own expert that *Emerald 1997* provides an explicit motivation to combine *Intrusive Activity 1991* demonstrates that SRI has failed to raise a genuine issue of material fact regarding motivation to combine.

a. SRI's "Evidence" of Secondary Considerations Does Not Preclude Summary Judgment

SRI also claims that evidence of "secondary considerations" (put forth by their expert) is sufficient to preclude summary judgment.[38] But this is not the law, even if the Court accepts all of these alleged facts in a light most favorable to SRI.[39] Summary judgment of obviousness is often appropriate even if the plaintiff presents evidence of secondary considerations of nonobviousness. *See Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 719 (Fed. Cir. 1991) (upholding summary judgment of obviousness where, although "secondary considerations weighed in favor of [patent owner]," summary judgment still was appropriate because "[t]he district court determined that secondary considerations did not carry sufficient weight to override a determination of obviousness based on primary considerations"); *Sandt Tech., Ltd. v. Resco Metal & Plastics Corp.*, 264 F.3d 1344, 1355 (Fed. Cir. 2001) (upholding summary judgment of obviousness and noting that "[w]e see no error in the district court's conclusion in this case that the secondary considerations cannot overcome the strong evidence of obviousness presented."); *see also Union Carbide Corp. v. American Can Co.*, 724 F.2d 1567, 1576 (Fed. Cir. 1984).

Here, what the parties dispute is the *ultimate legal conclusion of obviousness*, not the underlying facts. Accordingly, there is no issue of fact requiring a trial:

> [W]here the ultimate legal conclusion of obviousness is disputed, but not the

[38] Res. Br. at 30-31 [D.I. 339].

[39] Defendants do not present their disputes on these positions in this motion because the secondary considerations do not affect the outcome of the ultimate legal conclusion of obviousness.

> underlying facts, there is no issue of fact requiring a trial, even though some facts favor obviousness, some nonobviousness. This is so even in a case where a jury is demanded, because it is not the function of the jury to pick and choose among *established facts* relating to obviousness in contrast to its obligation to sift through *conflicting evidence* and determine what those facts are.

Newell Cos. v. Kenney Mfg. Co., 864 F.2d 757, 763 (Fed. Cir. 1988) (internal citations omitted).

The existence of evidence of secondary considerations "does not control the obviousness determination." *Richardson-Vicks Inc. v. Upjohn Co.*, 122 F.3d 1476, 1483 (Fed. Cir. 1997) (upholding summary judgment of obviousness in part because "[t]he unexpected results and commercial success of the claimed invention, although supported by substantial evidence, do not overcome the clear and convincing evidence that the subject matter sought to be patented is obvious"); *see also Motorola, Inc. v. Interdigital Tech. Corp.*, 121 F.3d 1461, 1472 (Fed. Cir. 1997). Here, the "secondary considerations cannot overcome the strong evidence of obviousness." *Sandt Tech.*, 264 F.3d at 1355. Indeed, SRI makes no attempt to explain why any of these secondary considerations would affect the explicit motivation to combine the references.

As SRI's expert conceded, *Emerald 1997* itself provides an express motivation to combine its teachings with the teachings of *Intrusive Activity 1991.*[40] Given this admitted express motivation to combine within SRI's own publication, summary judgment of invalidity under § 103 is appropriate.[41]

[40] Kesidis Tr. 673-76 [D.I. 301, Ex. V].

[41] SRI's behavior in discovery regarding secondary considerations should also prevent them from benefiting from such "facts." During fact discovery, SRI maintained in its Interrogatory Responses that Peter Neumann was the SRI employee most knowledgeable about secondary considerations. *See* SRI's Supplemental Response to Interrogatories No. 12 and No. 15 [No. 12], dated Dec. 15, 2005 (identifying Peter Neumann at page 2). [7/10/06 Godfrey Decl. Ex. WW]. But at his deposition on the last day of fact discovery, Mr. Neumann disclaimed all knowledge of any secondary considerations. Neumann Tr. 147-59 [7/10/06 Godfrey Decl. Ex. VV]. Only over a month *after* the close of fact discovery did SRI supplement its Interrogatory Responses and remove Mr. Neumann's name as the person most knowledgeable. *See* SRI's Supplemental Response to Symantec's Interrogatories Nos. 1, 12 (First Set of Interrogatories), 13 and 15 (Second Set of Interrogatories) [No. 12], dated May 5, 2006 (identifying Phillip